



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/635,389	08/06/2003	Wendell M. Smith	01251-P0011B	1191
24126 7590 06/12/2007 ST. ONGE STEWARD JOHNSTON & REENS, LLC 986 BEDFORD STREET STAMFORD, CT 06905-5619			EXAMINER SINGH, SATWANT K	
			ART UNIT 2625	PAPER NUMBER
			MAIL DATE 06/12/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

10/635,389

Applicant(s)

SMITH, WENDELL M.

Examiner

Satwant K. Singh

Art Unit

2625

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 06 August 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 August 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 8/06/03 and 03/13/07.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-4, 6, 7, 9, 12, 15-27, and 32 are rejected under 35 U.S.C. 102(e) as being anticipated by Stefik et al. (US 7,031,471).

3. Regarding Claim 1, Stefik et al disclose a document security system for printing secured documents comprising: a digital file (digital work) accessible by a receiver via a terminal (external interface for receiving and transmitting data) (col. 5, lines 46-49); a printer connected to the terminal (rendering device) (col. 6, lines 4-13); security data (watermark) specific to each page of said digital file (graphical symbol or printed notice that appears on each page) (col. 2, lines 1-7); and a mark (watermark) printed by said printer on each page of the printed digital file (page by page basis the position and shape of watermarks) (col. 10, lines 50-53), said mark containing data specific to each page of the printed digital file (glyph watermarks to carry document identification can be embedded by the publisher) (col. 10, lines 24-31).

4. Regarding Claim 2, Stefik et al disclose a document security system for printing secured documents wherein said printer is connected to said terminal via a network

Art Unit: 2625

connection (digital works are distributed from trusted systems to trusted rendering devices via computer networks) (col. 4, lines 58-60).

5. Regarding Claim 3, Stefik et al disclose a document security system for printing secured documents further comprising an identification device for identifying the sender (Fig. 5) (tags "Description" 501, "Work-ID" 502 and "Owner" 503 provide identification information for the digital work) (col. 8, lines 60-65).

6. Regarding Claim 4, Stefik et al disclose a document security system for printing secured documents wherein a second identification device (print right) is provided at the printer wherein the printer will not print (*it is interpreted by the examiner that if the printer repository does not have a print right, it will not decrypt the digital work*) said digital document unless identification data gathered by the second identification device matches stored identification data (Fig. 4, S406) of users that are allowed access to said digital document (Fig. 4, S407) (if the digital work has the print right, the printer repository decrypts the digital work and generates the watermark that will be printed on the digital work) (col. 7, lines 55-67, col. 8, lines 1-20).

7. Regarding Claim 6, Stefik et al disclose a document security system for printing secured documents wherein the security system encrypts said digital file prior to said digital file being sent to the printer (digital works and various communications are encrypted whenever they are transferred between repositories) (col. 6, lines 1-3).

8. Regarding Claim 7, Stefik et al disclose a document security system for printing secured documents wherein said mark is selected from the group consisting of: a

Watermark or an Optical Variable Device (the rendered work is watermarked to record data about the digital work and the rendering event) (col. 5, lines 1-7).

9. Regarding Claim 9, Stefik et al disclose a document security system for printing secured documents wherein the characteristics of said mark are selected from the group consisting of covert data (invisible watermark), overt data (visible watermark) or combinations thereof (multiple watermarking techniques) (col. 8, lines 32-36).

10. Regarding Claim 12, Stefik et al disclose a document security system for printing secured documents further comprising verification data gathered by the security system for verifying whether the sender (repository 1) has clearance access said digital file (Fig. 4, S401) (digital work is assigned usage rights) (col. 7, lines 60-65).

11. Regarding Claim 15, Stefik et al disclose a document security system for printing secured documents comprising: a digital file (digital work) accessible by a sender via a terminal (external interface for receiving and transmitting data) (col. 5, lines 46-49), said digital file comprising at least two pages to be printed (pages of a digital work) (col. 12, lines 15-16); a printer connected to the terminal via a network (rendering device) (col. 6, lines 4-13); security data (watermark) specific to each page of the digital file (graphical symbol or printed notice that appears on each page) (col. 2, lines 1-7); and at least two marks (visible and invisible watermarks) (col. 8, lines 30-45) printed by said printer on the at least two pages of the printed digital file (pages of a digital work) (col. 12, lines 15-16), said marks containing data specific to each of the at least two pages of the printed digital file (glyph watermarks to carry document identification can be embedded

by the publisher) (col. 10, lines 24-31) and said at least two marks being different from each other (visible versus invisible) (col. 8, lines 30-45).

12. Regarding Claim 16, Stefik et al disclose a document security system for printing secured documents further comprising verification data gathered by the security system for verifying whether the sender (repository 1) has clearance access said digital file (Fig. 4, S401) (digital work is assigned usage rights) (col. 7, lines 60-65).

13. Regarding Claim 17, Stefik et al disclose a document security system for printing secured documents wherein said verification data includes identification of the sender (Fig. 5) (tags "Description" 501, "Work-ID" 502 and "Owner" 503 provide identification information for the digital work) (col. 8, lines 60-65).

14. Regarding Claim 18, Stefik et al disclose a document security system for printing secured documents wherein the security system encrypts said digital file prior to said digital file being sent to said printer (digital works and various communications are encrypted whenever they are transferred between repositories) (col. 6, lines 1-3).

15. Regarding Claim 19, Stefik et al disclose a document security system for printing secured documents wherein said mark is a watermark (the rendered work is watermarked to record data about the digital work and the rendering event) (col. 5, lines 1-7).

16. Regarding Claim 20, Stefik et al disclose a document security system for printing secured documents wherein the characteristics of said mark are selected from the group consisting of covert data (invisible watermark), overt data (visible watermark) or combinations thereof (multiple watermarking techniques) (col. 8, lines 32-36).

17. Regarding Claim 21, Stefik et al disclose method for printing secured documents comprising the steps of: collecting verification data from a sender relating to a digital file (assigned usage rights) (col. 7, lines 55-67, col. 8, lines 1-20); verifying access to the digital file based upon the collected verification data (Fig. 4, S401) (digital work deposited into repository 1) (col. 7, lines 55-67, col. 8, lines 1-20); accessing the digital file (Fig. 4, S402 and S403) (repository 1 transfers a copy of the digital work to repository 2) (col. 7, lines 55-67, col. 8, lines 1-20); inputting a print command (Fig. 4, S404) (repository 2 receives a user request to print the digital work) (col. 7, lines 55-67, col. 8, lines 1-20); generating security data related to the verification data (watermark information to be placed on the digital work associated with the rendering or distribution event) (col. 8, lines 30-44), the security data being specific to each page of the digital file to be printed (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44); encrypting the digital file (digital works and various communications are encrypted whenever they are transferred between repositories) (col. 6, lines 1-3); sending the encrypted digital file to a printer (Fig. 4, S406) (printer repository receives the encrypted digital work) (col. 7, lines 55-67, col. 8, lines 1-20); and printing the digital file with a mark on each page of the document (Fig. 4, S408) (printer generates the watermark that will be printed on the digital work) (col. 7, lines 55-67, col. 8, lines 1-20), the mark for each page containing data specific to each page of the printed document (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44).

18. Regarding Claim 22, Stefik et al disclose a method for printing secured documents further comprising the steps of selectively granting the sender (repository 1) access to the digital file based upon the collected verification data (Fig. 4, S401) (digital work is assigned usage rights) (col. 7, lines 60-65).

19. Regarding Claim 23, Stefik et al disclose a method for printing secured documents wherein the verification data includes identification of the sender (Fig. 5) (tags "Description" 501, "Work-ID" 502 and "Owner" 503 provide identification information for the digital work) (col. 8, lines 60-65).

20. Regarding Claim 24, Stefik et al disclose a method for printing secured documents wherein the mark comprises a watermark (the rendered work is watermarked to record data about the digital work and the rendering event) (col. 5, lines 1-7).

21. Regarding Claim 25, Stefik et al disclose a method for printing secured documents wherein the characteristics of the mark are selected from the group consisting of covert data (invisible watermark), overt data (visible watermark) or combinations thereof (multiple watermarking techniques) (col. 8, lines 32-36).

22. Regarding Claim 26, Stefik et al disclose a method for printing secured documents comprising the steps of: accessing the digital file (Fig. 4, S402 and S403) (repository 1 transfers a copy of the digital work to repository 2) (col. 7, lines 55-67, col. 8, lines 1-20); generating security data (watermark) related to the digital file (watermark information to be placed on the digital work associated with the rendering or distribution event) (col. 8, lines 30-44), the security data being specific to each page of the digital



file to be printed (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44); sending the digital file to a printer (Fig. 8, S408) (printer repository transmits the decrypted digital file with the watermark to a printer device for printing) (col. 7, lines 55-67, col. 8, lines 1-20); printing the digital file and a mark on each page of the digital file (watermark information placed on the digital work), the mark containing data specific to each page of the printed digital file (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44).

23. Regarding Claim 27, Stefik et al disclose a document security system for printing secured documents comprising: a digital file (digital work) accessible by a receiver via a computer terminal (external interface for receiving and transmitting data) (col. 5, lines 46-49); security data specific to said digital file (watermark information to be placed on the digital work associated with the rendering or distribution event) (col. 8, lines 30-44) and to each page of said digital file (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44); a printer connected to the computer terminal (rendering device) (col. 6, lines 4-13); and a mark printed by said printer on each page of the printed digital file (watermark information placed on the digital work), said mark containing data specific to each page of the printed digital file (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44).

24. Regarding Claim 32, Stefik et al disclose a document security system for printing secured documents comprising: a digital file (digital work) accessible by a sender via a

Art Unit: 2625

terminal (external interface for receiving and transmitting data) (col. 5, lines 46-49); a printer connected to the terminal (rendering device) (col. 6, lines 4-13) via a network connection (digital works are distributed from trusted systems to trusted rendering devices via computer networks) (col. 4, lines 58-60); security data specific to each page of said digital file (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44); and a mark printed by said printer (printer repository transmits the decrypted digital file with the watermark to a printer device for printing) (col. 7, lines 55-67, col. 8, lines 1-20) on each page of the printed digital file (watermark information placed on the digital work), said mark containing data specific to each page of the printed digital file (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44).

***Claim Rejections - 35 USC § 103***

25. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

26. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stefik et al. in view of Carr et al. (US 6,389,151).

27. Regarding Claim 5, Stefik et al fail to teach a document security system for printing secured documents wherein said identification device comprises a fingerprint keypad.

Carr et al teach a document security system for printing secured documents wherein said identification device comprises a fingerprint keypad (Fig. 3, fingerprint reader 303) (col. 4, lines 63-65).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teaching of Stefik with the teaching of Carr to allow a user to use their fingerprint as identification to print secure documents.

28. Claims 8, 11, 28, 29, 30, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stefik et al. in view of Zorab et al. (US 2003/0177095).

29. Regarding Claim 8, Stefik et al fail to teach a document security system for printing secured documents wherein said mark comprises DNA information coded in ink utilized to print said mark.

Zorab et al teach a document security system for printing secured documents wherein said mark comprises DNA information coded in ink utilized to print said mark (DNA tag) (page 2, paragraph [0019]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Zorab to encode one's DNA tag in the watermark information.

30. Regarding Claim 11, Stefik et al fail to teach a document security system for printing secured documents wherein said printer uses ink to print said digital file, said ink selected from the group consisting of: DNA ink or fluorescent ink.

Zorab et al teach a document security system for printing secured documents wherein said printer uses ink to print said digital file, said ink selected from the group

Art Unit: 2625

consisting of: DNA ink or fluorescent ink (fluorescent ink or DNA tag) (page 2, paragraph [0019]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Zorab to encode the watermark information using a DNA tag or fluorescent ink.

31. Regarding Claim 28, Stefik et al teach a document security system for printing secured documents comprising: a digital file (digital work) accessible by a receiver via a computer (external interface for receiving and transmitting data) (col. 5, lines 46-49); a printer connected to the computer (rendering device) (col. 6, lines 4-13); security data specific to said digital file (watermark information to be placed on the digital work associated with the rendering or distribution event) (col. 8, lines 30-44); and a mark printed by said printer with said ink on the printed digital file, said mark containing data specific the printed digital file (watermark information placed on the digital work) (col. 8, lines 30-44).

Stefik et al fail to teach a document security system for printing secured documents comprising: ink usable by said printer, said ink having coded DNA information that contains said security data specific to said digital file.

Zorab et al teach a document security system for printing secured documents comprising: ink usable by said printer, said ink having coded DNA information that contains said security data specific to said digital file (DNA tag) (page 2, paragraph [0019]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Zorab to encode one's DNA tag in the watermark information.

32. Regarding Claim 29, Stefik et al teach a document security system for printing secured documents wherein said security data further comprises data specific to each page of said digital file and said mark further contains data specific to each page of said digital file (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44).

33. Regarding Claim 30, Stefik et al teach a document security system for printing secured documents comprising: a digital file (digital work) accessible by a receiver via a computer (external interface for receiving and transmitting data) (col. 5, lines 46-49); a printer connected to the computer; security data specific to said digital file (rendering device) (col. 6, lines 4-13); and a watermark printed by said printer on each page of the printed digital file (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44), said watermark containing data specific the printed digital file (watermark information to be placed on the digital work associated with the rendering or distribution event) (col. 8, lines 30-44).

Stefik et al fail to teach a document security system for printing secured documents wherein the watermark is an Optical Variable Device.

Zorab et al teach document security system for printing secured documents wherein the watermark is an Optical Variable Device (optical device such as a hologram or digitally printed device) (page 2, paragraph [0019]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Zorab to encode the watermark information in a hologram.

34. Regarding Claim 31, Stefik et al teach a document security system for printing secured documents wherein said security data further comprises data specific to each page of said digital file and said watermark further contains data specific to each page of said digital file (watermark information can be extended to include the entire distribution chain of the digital work) (col. 8, lines 39-44).

Stefik et al fail to teach document security system for printing secured documents wherein the watermark is an Optical Variable Device.

Zorab et al teach document security system for printing secured documents wherein the watermark is an Optical Variable Device (optical device such as a hologram or digitally printed device) (page 2, paragraph [0019]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Zorab to encode the watermark information in a hologram.

35. Claims 10, 13, and 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Stefik et al. in view of Martin et al. US 5,710,420).

Regarding Claim 10, Stefik et al fail to teach a document security system for printing secured documents wherein said mark is printed on a medium, said medium selected from the group consisting of: plain paper, paper having a distinct pattern located thereon, or thermal transfer holographic foil.

Martin et al teach a document security system for printing secured documents wherein said mark is printed on a medium, said medium selected from the group consisting of: plain paper, paper having a distinct pattern located thereon, or thermal transfer holographic foil (protochromic marking material can be applied to any desired substrate, for example plain papers, ruled papers, bond paper, etc) (col. 8, lines 59-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Stefik with the teaching of Martin to allow a user to embed watermark information on many types of media.

36. Regarding Claim 13, Stefik et al. teaches a document security system for printing secured documents wherein said verification data includes identification of the sender (Fig. 5) (tags "Description" 501, "Work-ID" 502 and "Owner" 503 provide identification information for the digital work) (col. 8, lines 60-65).

37. Regarding Claim 14, Stefik et al teaches a document security system for printing secured documents wherein the security system selectively grants the user access to said digital file based upon the collected verification data (print right) (col. 8, lines 9-20).

### ***Conclusion***

38. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Claiborne (US 6,765,688) discloses a method of defining watermark for both print and copy.

Rhoads et al. (US 7,136,502) discloses stationery or other printable media that is encoded with a digital watermark.

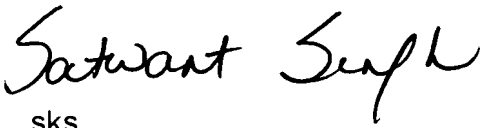
Tame (US 2004/0026502) discloses a method and system for transferring verification data from a first carrier to at least a second carrier in a secure manner.

**Contact Information**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Satwant K. Singh whose telephone number is (571) 272-7468. The examiner can normally be reached on Monday thru Friday 8am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David K. Moore can be reached on (571) 272-7437. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

  
sks

Satwant K. Singh  
Examiner  
Art Unit 2625



DAVID MOORE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2600